ECSS-Q-ST-40C
6 March 2009

Space product assurance

Safety

ECSS Secretariat
ESA-ESTEC
Requirements & Standards Division
Noordwijk, The Netherlands

Foreword

This Standard is one of the series of ECSS Standards intended to be applied together for the management, engineering and product assurance in space projects and applications. ECSS is a cooperative effort of the European Space Agency, national space agencies and European industry associations for the purpose of developing and maintaining common standards. Requirements in this Standard are defined in terms of what shall be accomplished, rather than in terms of how to organize and perform the necessary work. This allows existing organizational structures and methods to be applied where they are effective, and for the structures and methods to evolve as necessary without rewriting the standards.

This Standard has been prepared by the ECSS-Q-ST-40C Working Group, reviewed by the ECSS Executive Secretariat and approved by the ECSS Technical Authority.

Disclaimer

Published by: ESA Requirements and Standards Division
ESTEC, P.O. Box 299,
2200 AG Noordwijk
The Netherlands

Change log

ECSS-Q-40A 19 April 1996	First issue
ECSS-Q-40B 17 May 2002	Second issue
ECSS-Q-ST-40C 6 March 2009	Third issue The main changes between ECSS-Q-40B and the current version are the following: • Complete and thorough review of ECSS-Q-40B with the focus on simplification and streamlining to improve clarity and consistency of requirements. • Applicability guidelines of ECSS-Q-ST-40 to the different space systems has been defined (see applicability matrix provided in Annex E). • System safety programme requirements reworked, i.e. the system safety programme supports the risk management process described in ECSS-M-ST-80. • Space debris mitigation streamlined. • Atmospheric re-entry addressed. • Safety design principles reworked. • Safety risk reduction and control updated. • Safety analysis requirements and techniques updated. • Common scheme for consequence severity classification used in ECSS-Q-ST-30C and ECSS-Q-ST-40C. • Identification and control of safety-critical functions updated. • Established link to ECSS standard on “Critical-item control” (ECSS-Q-ST-10-04). • Harmonized ECSS-Q-ST-40C with associated Level 3 standards. • Informative annex on European legislation and ‘CE’ marking added (Annex F). • DRDs revisited and updated. • Document reworked to be in compliance with ECSS standards drafting rules.

Table of contents

Change log **3**

1 Scope **8**

2 Normative references **9**

3 Terms, definitions and abbreviated terms **10**

3.1 Terms from other standards 10

3.2 Terms specific to the present standard 10

3.3 Abbreviated terms 12

4 Safety principles **14**

4.1 Objective 14

4.2 Policy 14

4.2.1 General 14

4.2.2 Implementation 14

4.3 Safety programme 15

5 Safety programme **16**

5.1 Scope 16

5.2 Safety programme plan 16

5.3 Conformance 16

5.4 Safety organization 17

5.4.1 Safety manager 17

5.4.2 Safety manager access and authority 17

5.4.3 Safety audits 18

5.4.4 Approval of documentation 18

5.4.5 Approval of hazardous operations 18

5.4.6 Representation on boards 18

5.4.7 Safety approval authority 18

5.5 Safety risk assessment and control 19

5.6 Safety critical items 19

5.7 Project phases and safety review cycle 19

5.7.1 Safety program tasks and reviews 19
5.7.2 Progress meetings 23
5.7.3 Safety reviews 23
5.8 Safety compliance demonstration 23
5.9 Safety training 24
5.9.1 General 24
5.9.2 Product specific training 24
5.9.3 General awareness briefings 24
5.9.4 Basic technical training 25
5.9.5 Training records 25
5.10 Accident-incident reporting and investigation 25
5.11 Safety documentation 25
5.11.1 General 25
5.11.2 Safety data package 25
5.11.3 Safety deviations and waivers 26
5.11.4 Safety lessons learned 27
5.11.5 Documentation of safety critical items 27

6 Safety engineering 28

6.1 Overview 28
6.2 Safety requirements identification and traceability 28
6.3 Safety design objectives 28
6.3.1 Safety policy and principles 28
6.3.2 Design selection 28
6.3.3 Hazard reduction precedence 29
6.3.4 Environmental compatibility 31
6.3.5 External services 31
6.3.6 Hazard detection - signalling and safing 31
6.3.7 Space debris mitigation 32
6.3.8 Atmospheric re-entry 32
6.3.9 Safety of Earth return missions 32
6.3.10 Safety of human spaceflight missions 33
6.3.11 Access 33
6.4 Safety risk reduction and control 33
6.4.1 Severity of hazardous event 33
6.4.2 Failure tolerance requirements 35
6.4.3 Design for minimum risk 36
6.4.4 Probabilistic safety targets 37

6.5 Identification and control of safety-critical functions 38
6.5.1 Identification 38
6.5.2 Inadvertent operation 38
6.5.3 Status information 38
6.5.4 Safe shutdown and failure tolerance requirements 38
6.5.5 Electronic, electrical, electromechanical components 38
6.5.6 Software functions 39
6.6 Operational Safety 39
6.6.1 Basic requirements 39
6.6.2 Flight operations and mission control 40
6.6.3 Ground operations 41

7 Safety analysis requirements and techniques 43
7.1 Overview 43
7.2 General 43
7.3 Assessment and allocation of requirements 44
7.3.1 Safety requirements 44
7.3.2 Additional safety requirements 44
7.3.3 Define safety requirements - functions 44
7.3.4 Define safety requirements - subsystems 44
7.3.5 Justification 44
7.3.6 Functional and subsystem specification 44
7.4 Safety analyses during the project life cycle 44
7.5 Safety analyses 45
7.5.1 General 45
7.5.2 Hazard analysis 45
7.5.3 Safety risk assessment 46
7.5.4 Supporting assessment and analysis 46

8 Safety verification 50
8.1 General 50
8.2 Hazard reporting and review 50
8.2.1 Hazard reporting system 50
8.2.2 Safety status review 50
8.2.3 Documentation 50
8.3 Safety verification methods 51
8.3.1 Verification engineering and planning 51
8.3.2 Methods and reports 51
8.3.3 Analysis 51

8.3.4 Inspections 51
8.3.5 Verification and approval 52
8.4 Verification of safety-critical functions 52
8.4.1 Validation 52
8.4.2 Qualification 52
8.4.3 Failure tests 53
8.4.4 Verification of design or operational characteristics 53
8.4.5 Safety verification testing 53
8.5 Hazard close-out 53
8.5.1 Safety assurance verification 53
8.5.2 Hazard close-out verification 54
8.6 Declaration of conformity of ground equipment 54

Annex A (informative) Analyses applicability matrix 55

Annex B (normative) Safety programme plan - DRD 57

Annex C (normative) Safety verification tracking log (SVTL) DRD 59

Annex D (normative) Safety analysis report including hazard reports - DRD 63

Annex E (informative) Criteria for probabilistic safety targets 65

Annex F (informative) Applicability guidelines 66

Annex G (informative) European legislation and 'CE' marking 72

Bibliography 75

Tables

Table 6-1: Severity of consequences 35

1
Scope

This Standard defines the safety programme and the safety technical requirements aiming to protect flight and ground personnel, the launch vehicle, associated payloads, ground support equipment, the general public, public and private property, the space system and associated segments and the environment from hazards associated with European space systems.

This Standard is applicable to all European space projects.

This standard may be tailored for the specific characteristic and constraints of a space project in conformance with ECSS-S-ST-00.

2
Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this ECSS Standard. For dated references, subsequent amendments to, or revision of any of these publications do not apply. However, parties to agreements based on this ECSS Standard are encouraged to investigate the possibility of applying the more recent editions of the normative documents indicated below. For undated references, the latest edition of the publication referred to applies.

ECSS-S-ST-00-01	ECSS system – Glossary of terms
ECSS-E-ST-10	Space engineering – System engineering general requirements
ECSS-E-ST-32-01	Space engineering – Fracture control
ECSS-E-ST-32-10	Space engineering – Structural factors of safety for spaceflight hardware
ECSS-E-ST-40	Space engineering – Software general requirements
ECSS-M-ST-10	Space project management – Project planning and implementation
ECSS-M-ST-40	Space project management – Configuration and information management
ECSS-M-ST-80	Space project management – Risk management
ECSS-Q-ST-10	Space product assurance – Product assurance management
ECSS-Q-ST-10-04	Space product assurance – Critical-item control
ECSS-Q-ST-20	Space product assurance – Quality assurance
ECSS-Q-ST-30	Space product assurance – Dependability
ECSS-Q-ST-60	Space product assurance – Electrical, electronic and electromechanical (EEE) components
ECSS-Q-ST-70	Space product assurance – Materials, mechanical parts and processes
ECSS-Q-ST-80	Space product assurance – Software product assurance

3
Terms, definitions and abbreviated terms

3.1 Terms from other standards

For the purpose of this Standard, the terms and definitions from ECSS-S-ST-00-01 apply (see in clause 3.2 differences for "fail-safe" and "system"), in particular for the following terms:

accident

failure

hazard

NOTE (Specific to this Standard) Hazards are potential threats to the safety of a system. They are not events.

hazardous event

inhibit

risk

safety

NOTE (Specific to this Standard) Spacecraft is part of flight system

safety-critical function

3.2 Terms specific to the present standard

3.2.1 cause

action or condition by which a hazardous event is initiated (an initiating event)

NOTE 1 The cause can arise as the result of failure, human error, design inadequacy, induced or natural environment, system configuration or operational mode(s).

NOTE 2 This definition is specific to this Standard, when used in the context of hazard analysis.

3.2.2 fail-safe

design property of a system (or part of it), which prevents its failures from resulting in critical or catastrophic consequences

NOTE This definition is specific to this Standard (different from ECSS-S-ST-00-01), for use in the context of safety analysis.

3.2.3 hazard control

preventive or mitigation measure, associated to a hazard scenario, which is introduced into the system design and operation to avoid the events or to interrupt their propagation to consequence

3.2.4 hazardous command

command that can remove an inhibit to a safety-critical function or activate a hazardous subsystem

3.2.5 hazard reduction

process of elimination or minimization and control of hazards

3.2.6 hazard scenario

sequence of events leading from the initial cause to the unwanted safety consequence

NOTE The cause can be a single initiating event, or an additional action or a change of condition activating a dormant problem.

3.2.7 likelihood

probability of occurrence or the measure for the occurrence rate

3.2.8 operator error

failure of an operator to perform an action as required or trained or the inadvertent or incorrect action of an operator

[ISO 14620-1]

3.2.9 safety approval authority

entity that defines or makes applicable, for a given project, detailed technical safety requirements, and reviews their implementation

3.2.10 safety audit

independent examination to determine whether the procedures specific to the safety requirements are implemented effectively and are suitable to achieve the specified objectives

3.2.11 safety risk

measure of the threat to safety posed by the hazard scenarios and their consequences

NOTE 1 Safety risk is always associated with a specific hazard scenario or a particular set of scenarios. The risk posed by a single scenario is called individual scenario risk. The risk posed by a set of scenarios with the same top consequence is called overall risk.

NOTE 2 The magnitude of a safety risk is a combination of the severity and the likelihood of the consequence.

3.2.12 safety status parameter

parameter that makes it possible to assess the status of an implemented hazard control

3.2.13 system

set of interdependent elements constituted to achieve a given objective by performing a specified function

[IEC 50:1992]

NOTE The system is considered to be separated from the environment and other external systems by an imaginary surface which cuts the links between them and the considered system. Through these links, the system is affected by the environment, is acted upon by the external systems, or acts itself on the environment or the external systems.

3.2.14 system safety

application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle

[ISO 14620-1]

3.3 Abbreviated terms

For the purpose of this Standard, the abbreviated terms from ECSS-S-ST-00-01 and the following apply:

Abbreviation	Meaning
AR	acceptance review
CCB	configuration control board
CDR	critical design review

CRR	commissioning result review
EEE	electronic, electrical, electromechanical
ELR	end-of-life review
FMEA	failure modes and effects analysis
FMECA	failure modes, effects and criticality analysis
FRR	flight readiness review
FTA	fault tree analysis
GSE	ground support equipment
IEC	International Electrotechnical Commission
LRR	launch readiness review
MIP	mandatory inspection point
NRB	nonconformance review board
NUREG-CR	US Nuclear Regulatory Commission contractor report
ORR	operational readiness review
PDR	preliminary design review
PRR	preliminary requirements review
QR	qualification review
SRR	system requirements review
SVTL	safety verification tracking log
TRB	test review board

4
Safety principles

4.1 Objective

The objective of safety assurance is to ensure that all safety risks associated with the design, development, production and operations of space product are adequately identified, assessed, minimized, controlled and finally accepted through the implementation of a safety assurance programme.

4.2 Policy

4.2.1 General

The ECSS safety policy is to:

- ensure that space systems do not cause a hazard to, in order of priority:
  - human life,
  - the environment,
  - public and private property (including launch facilities),
  - spacecraft and launcher,
  - ground support equipment and facilities,
- determine and evaluate the safety risks associated with project activities,
- minimize safety risks in a technically effective and cost effective manner,
- ensure adequate verification of safety control measures.

4.2.2 Implementation

The ECSS safety policy is implemented by applying a safety programme which ensures that:

- safety is designed into the system,
- safety controls are adequately implemented in the verification plan,
- safety requirements including launch centre safety regulations are met,
- hazards are identified, and eliminated or, where this is not possible, minimized, ranked and controlled in accordance with project objectives in a manner acceptable to the customer and to the safety organisations involved in the implementation of the mission.

4.3 Safety programme

The safety programme comprises the:

- identification and control of all safety related risks with respect to the design, development and operations of space products,
- assessment of the risks based on qualitative and quantitative analysis as appropriate,
- application of a hazard reduction precedence and of control measures of the residual risks.

5
Safety programme

5.1 Scope

a. The supplier shall establish and maintain a safety programme to assure conformance with project safety policy and requirements.

b. The safety programme shall establish a safety management system to implement provisions of this Standard - commensurate with the programme requirements and tailored by the customer

NOTE 1 For tailoring, refer to clause 1.

NOTE 2 The system safety programme requirements are subject to tailoring, without diminishing the intent to protect flight and ground personnel, the launch vehicle, associated payloads, ground support equipment, the general public, public and private property, the space system and associated segments and the environment from hazards associated with space systems.

NOTE 3 As support to tailoring, informative Annex F provides a guideline for determining the applicability of this standard depending on the type of project.

5.2 Safety programme plan

a. The supplier shall establish and maintain a safety programme plan in conformance with the DRD in Annex B.

NOTE The plan can either be included as part of an overall project product assurance plan or as a separate safety programme plan.

b. The supplier shall cover, in his safety programme plan, the safety tasks for the project phases in conformance with 5.7.1.

5.3 Conformance

a. The supplier shall comply with all applicable national or international safety regulations.

b. The launch site safety regulations and rules shall be applied.

c. The implementation of safety requirements shall not be compromised by other requirements.

NOTE For example: security requirements.

5.4 Safety organization

5.4.1 Safety manager

a. Each supplier shall appoint a safety manager who has appropriate training or experience.

b. The safety manager shall have organisational authority and independence to:

1. establish and maintain a safety programme in accordance with the project safety requirements,

2. manage all safety assurance aspects of the design of the system (including software) and its operation in accordance with the Safety Plan,

3. coordinate the interfaces:

(a) with the relevant bodies involved in the project in accordance with the safety plan,

(b) with the safety launcher authority.

NOTE Depending on the project safety criticality, the safety manager can be combined with other functions (e.g. PA manager) when agreed with the customer.

5.4.2 Safety manager access and authority

5.4.2.1 Access

a. The safety manager shall:

1. have the right of access to safety-related data relevant to project safety in conformance with ECSS-M-ST-40,

2. have unimpeded access to any management level without organizational constraint on any aspect of project safety.

5.4.2.2 Authority

a. The safety manager or safety relevant authority shall have the authority to:

1. reject any project document, or to stop any project activity that does not conform to approved safety requirements or procedures,

2. interrupt hazardous operations when it becomes clear by the Safety Manager that the operation does not conform to the agreed measures defined in the corresponding hazard report and derived approved hazard procedure.

5.4.3 Safety audits

a. The supplier shall perform safety audits or reviews to verify compliance to project safety policy and requirements.

b. The safety audits shall be in accordance with ECSS-M-ST-10 and ECSS-Q-ST-10.

NOTE The safety audits can be part of the project audits.

c. The customer shall be informed of the audit schedule.

5.4.4 Approval of documentation

a. Documentation related to safety shall be approved by the safety manager upon his verification of completeness, compliance with stated safety requirements and formal closeout of open safety verification items (as defined and agreed during safety audits and reviews).

5.4.5 Approval of hazardous operations

a. The safety manager (or a designated representative) shall have concluded the review of, and approved, any hazardous operation before it is executed.

5.4.6 Representation on boards

a. The safety manager or designated delegate shall be represented at configuration control boards (CCBs), nonconformance review boards (NRBs), test review board (TRBs), and at qualification, and acceptance reviews, where safety requirements and safety-critical functions are involved.

b. The safety function shall be further represented at all boards dealing with health matters where exposure or endurance limits are defined for flight and ground crews.

5.4.7 Safety approval authority

a. The safety approval authority shall:

1. review and disposes the safety data submittals,
2. approve the close-out of hazards,
3. decide on deviations and waivers, and finally
4. accept the statement of safety compliance.

5.5 Safety risk assessment and control

a. The safety risk identification, reduction and control shall be part of the project's risk management process as specified in ECSS-M-ST-80.

b. Safety risk identification, reduction and control shall be a continuous and iterative process throughout the project life cycle, encompassing

1. allocation of safety requirements;
2. hazard and safety risk identification;
3. evaluation (including categorisation) of consequence severity;
4. hazard and safety risk reduction and control;
5. close out and acceptance of residual risk.

c. For the identification of hazards and associated safety risks, consideration shall be given to past experience, studies, ground and flight tests, reviews, the industrial process as well as the operational use.

5.6 Safety critical items

a. The safety critical items shall be part of the project's overall critical items control programme as specified in ECSS-Q-ST-10-04.

5.7 Project phases and safety review cycle

5.7.1 Safety program tasks and reviews

5.7.1.1 Mission analysis/Needs identification - Phase 0

a. Safety analysis shall support the identification of sources of safety risk as well as the performance of preliminary trade-off analyses between alternative system concepts.

b. The following safety programme tasks shall apply for human spaceflight programmes and safety critical systems:

1. Analyse safety requirements and lessons-learnt associated with similar previous missions;
2. Perform preliminary hazard analysis of the proposed system and operations concept to support concept trade-offs;
3. Perform comparative safety risk assessment of the concept options;
4. Identify the relevant project safety requirements;
5. Plan safety activities for the feasibility phase;
6. Support the mission definition review.

NOTE These tasks should also serve as a guideline for other space programmes.

5.7.1.2 Feasibility - Phase A

a. Safety analysis shall support trade-off analyses in arriving at the concept that has acceptable safety risk considering the project and mission constraints.

b. The design technology selected and the operational concept to be implemented shall be selected based on the analysis data for the safest system architecture to eliminate or reduce hazards to acceptable levels.

c. The following safety programme tasks shall apply for human spaceflight programmes and safety critical systems:

1. Commence hazard analyses of the design and operations concepts in order to identify applicable system level hazards, hazardous conditions, and potential hazardous events and consequences;
2. Support concept trades by identifying safety critical aspects of the concept options;
3. Apply hazard elimination and minimization and make safety recommendations;
4. Perform comparative safety risk assessments of the concept options;
5. Identify system level safety critical functions;
6. Identify system level project specific safety requirements;
7. Plan safety activities for the project definition phase;
8. Support the preliminary requirements review.

NOTE These tasks should also serve as a guideline for other space programmes.

5.7.1.3 Preliminary definition - Phase B

a. The safety analysis shall support a continued and more detailed safety optimization of the system design and operations and the identification of technical safety requirements and their applicability.

b. The analysis shall also provide inputs to safety risk assessment in support of safety risk evaluation, the identification of risk contributors in the design and in the operational concept.

c. The following safety programme tasks shall apply for human spaceflight programmes and safety critical systems:

1. Update hazard analysis in support of design and mission concept definition activities; identify additional project specific safety requirements;
2. Update safety critical functions identification, and define the failure tolerance requirements;
3. Identify emergency, warning, and caution situations;
4. Update the system safety risk assessment as part of the contribution provided by the safety domain to the risk management process;

5. Identify project safety requirements;
6. Ensure that project requirement documentation and activities comply with project safety requirements;
7. Support a system requirements review and preliminary design review;
8. Plan verification of safety requirements implementation;
9. Prepare the safety plan for the detailed definition, production and qualification phase.

NOTE These tasks should also serve as a guideline for other space programmes.

5.7.1.4 Detailed definition, production and qualification testing - Phase C/D

a. Safety analysis shall support detailed design, production, qualification, testing.

b. Safety analysis shall also support operational safety optimization, safety requirements implementation evaluation, risk reduction verification, and hazard and risk acceptance.

c. Analysis of operations shall also support the identification of emergency and contingency response planning and training requirements, and the development of procedures.

d. The following safety programme tasks shall apply for human spaceflight programmes and safety critical systems:
   1. Perform detailed system level hazard analysis;
   2. Perform supporting safety analysis;
   3. Update the project technical safety requirements to incorporate the results of safety analyses;
   4. Ensure that the project implementation and verification programme covers identified hazard control verification activities;

      NOTE For example: reviews, inspections, analyses and tests.

   5. Update safety critical functions identification, failure tolerance requirements, and identify safety critical items;
   6. Implement control programme for safety critical items;
   7. Perform safety risk assessment in support of design improvement, project resource apportionment, control programme for safety critical items and project reviews;
   8. Monitor verification of safety requirements implementation;
   9. Verify and document hazard control implementation;
   10. Check that all open verification items are recorded and agreed procedures are in place;
   11. Support the critical design review, the qualification review and the acceptance review;

12. Perform project internal safety reviews and internal audits;
13. Identify, monitor and control project assembly, integration, testing and handling operations which are potentially hazardous to personnel or hardware;
14. Review and approve hazardous and safety critical operational procedures;
15. Perform accident-incident reporting and investigation;
16. Support customer safety reviews at defined programme milestones;
17. Prepare a project safety "lessons-learned" report;
18. Prepare operational phase safety plan.

NOTE These tasks should also serve as a guideline for other space programmes.

5.7.1.5 Utilization - Phase E

a. Safety analysis shall evaluate design and operational changes for impact to safety, assuring that safety margins are maintained and that operations are conducted within accepted risk.

b. The analysis shall also support the evaluation of operational anomalies for impact to safety, and the continued evaluation of risk trends.

c. The following safety programme tasks shall apply for human spaceflight programmes and safety critical systems:

1. Issue the operational phase safety plan;
2. Review operational procedures;
3. Approve safety critical operational procedures;
4. Identify and monitor hazardous operations;
5. Support the flight readiness review, operational readiness review, launch readiness review and flight qualification reviews;
6. Support ground and flight operations;
7. Perform safety critical items control;
8. Monitor and assess evolution of the system configuration and operations resulting from design fixes and updates;
9. Update hazard analyses and implement additional hazard controls as necessary;
10. Investigate safety related flight anomalies and trends;
11. Update safety risk assessment as necessary to support operational decisions;
12. Prepare disposal phase safety plan.

NOTE These tasks should also serve as a guideline for other space programmes.

5.7.1.6 Disposal - Phase F

a. Safety analysis shall evaluate all disposal operations and associated hazards.

b. Disposal solutions shall be identified which meet the project's safety requirements.

c. The following safety programme tasks shall apply for human spaceflight programmes and safety critical systems:

1. Perform hazard analysis with respect to the disposal operations;
2. Check that the disposal operation conforms to international safety regulations by performing the necessary safety analysis;
3. Review the procedures of the disposal operations;
4. Support the mission close-out review.

NOTE These tasks should also serve as a guideline for other space programmes.

5.7.2 Progress meetings

a. The supplier shall hold regular safety status and progress meetings with the customer and his lower tier suppliers as part of the project progress meetings as specified in ECSS-M-ST-10.

b. The relevant customer and supplier specialists shall attend the meetings.

5.7.3 Safety reviews

a. The customer shall define, conduct and chair the safety reviews to ensure satisfactory implementation of safety programme and technical safety requirements.

NOTE A supplier is considered as a customer vis-à-vis its lower tier suppliers (as defined in ECSS-S-ST-00).

b. The supplier shall support safety reviews by the customer and the relevant safety approval authority, as specified in the relevant review plans.

c. Each supplier participating in a safety review shall prepare, and submit for review, the safety data package.

d. Safety reviews shall be performed, and the review objectives achieved, in conformance with clause 5.7.1.

5.8 Safety compliance demonstration

a. The supplier shall provide a statement of safety compliance to demonstrate that the space system elements conform to stated safety requirements.

b. The supplier shall include in his statement of compliance a statement that open verifications are followed up in the safety verification tracking log (SVTL), as defined in clause 8.5.1, and do not affect further safe processing.

c. The project shall provide to the safety approval authority all safety-related information for their acceptance of the statement of safety compliance.

5.9 Safety training

5.9.1 General

a. Safety training shall be part of the overall training in accordance with ECSS-Q-ST-20.

b. All safety related training of any personnel working - permanently or occasionally - with system elements that can have hazardous properties shall have three major aspects:

1. general awareness briefings on safety measures to be taken at a given location or working environment;

2. basic technical training in the required safety techniques and skills which is a prerequisite to fulfil the job function under consideration;

NOTE For example: inspection, test, maintenance or integration.

3. product specific training that focuses on the hazards related to the specific system element.

5.9.2 Product specific training

a. The supplier shall identify the need for product specific safety training and implement the corresponding safety training programme for all relevant parties.

b. The supplier shall inform the customer of any safety training identified by him as necessary for the flight operations crew or mission control personnel, together with a definition of the type of training required and its scope.

c. The supplier shall support the implementation of the customer's training programme for the flight operations crew or mission control personnel.

5.9.3 General awareness briefings

a. All personnel accessing the area where the product is processed shall participate previously in the general safety awareness briefing.

5.9.4 Basic technical training

a. The supplier shall provide basic technical training to all project engineering and safety personnel working with hazardous products.

5.9.5 Training records

a. The supplier shall maintain records of personnel having received safety training in accordance with ECSS-Q-ST-20.

5.10 Accident-incident reporting and investigation

a. The supplier shall report to the customer all accidents and incidents occurred during project activities under the control of the supplier or his lower tier suppliers that affect the system element.

b. The supplier shall support - at request - project related accident and incident investigations that occur outside of the supplier's control or facility.

c. The supplier shall coordinate the investigation activities in cooperation with other supplier functional departments and lower tier suppliers.

d. The accident or incident investigation report shall be formally closed by the supplier upon approval by the customer.

e. If the conclusion of the assessment is that the accident-incident has had an effect on the project, i.e. the safety of the product or its operation, the organisations safety representative shall be informed.

f. In case of 5.10e., the accident-incident report shall become part of the project's safety data and is documented in the safety data package.

5.11 Safety documentation

5.11.1 General

a. The supplier shall maintain, as part of the project documentation, all safety-related data to support reviews and safety compliance demonstration.

b. The customer shall be given access to this data on request during audits, safety reviews and meetings held at the supplier's premises in accordance with ECSS-M-ST-40.

5.11.2 Safety data package

a. The supplier shall submit a safety data package (SDP) to support reviews.

NOTE This can be a stand-alone package or be integrated into the overall data package if the

safety review is part of an overall project review.

b. The safety data package shall contain at least the following safety related documentation:

1. Safety analysis report (in accordance with Annex D);
2. Supporting analysis (if applicable);
3. Safety risk assessment (if applicable);
4. Hazardous ground operations list and procedures;
5. Safety verification tracking log (SVTL, in accordance with Annex C).

c. The contents of the safety data packages for the planned safety reviews of a project or programme shall be specified by the Safety Approval Authority to assure they support the objectives of the safety reviews for which they are delivered (in conformance with clause 5.7.2).

d. The supplier shall use the actual configuration baseline, as defined by ECSS-M-ST-40, as the design and operational baseline that is the subject of the safety data package.

e. The supplier shall integrate safety data related to the various subsystems or equipment that makes up the system into the safety data package that is presented at the review.

f. All safety data shall be traceable from the safety data package and available for review.

5.11.3 Safety deviations and waivers

5.11.3.1 Request for deviation or waiver

a. Safety requirements that cannot be met shall be identified as specified in ECSS-M-ST-40.

b. A request for deviation or waiver shall be generated and tracked according to the requirements of ECSS-M-ST-40.

5.11.3.2 Assessment of deviation or waiver

a. All RFD/RFW shall be assessed in order to identify those which impact safety.

b. The accumulated deviations and waivers that affect safety shall be assessed to ensure that the effects of individual deviations do not invalidate the rationale used for the acceptance of other deviations.

5.11.3.3 Acceptance by the safety approval authority

a. Safety deviations and waivers shall be subject to safety approval authority acceptance.

5.11.3.4 Review and disposition

a. Deviations and waivers that affect project safety requirements or safety-critical functions which the supplier considers acceptable shall be subject of review and disposition by the customer and the safety approval authority.

5.11.4 Safety lessons learned

a. Safety lessons learned shall be collected during the project and used during the project, as far as they are relevant.

NOTE Safety lessons learned should consider as a minimum:

- the impact of newly imposed requirements;
- assessment of all malfunctions, accidents, anomalies, deviations and waivers;
- effectiveness of safety strategies of the project;
- new safety tools and methods that have been developed or demonstrated;
- effective versus ineffective verifications that have been performed;
- changes proposed to safety policy, strategy or technical requirements with rationale.

b. The safety lessons learned information shall be made available to the customer and suppliers, particularly to project and safety managers as well as design and safety engineers upon request for use on other projects.

5.11.5 Documentation of safety critical items

a. The safety critical items identified by the safety analysis shall be documented in accordance with ECSS-Q-ST-10-04.

6
Safety engineering

6.1 Overview

Safety is an integral part of all project product assurance and engineering activities. It is not a stand-alone activity. The quality of all safety engineering related work is based on assurance that the system is designed, qualified, manufactured, and operated in accordance with the ECSS product assurance requirements.

Safety engineering consists of safety analysis, management of hazard and risk reduction processes, hazard and risk potential assessment, design assurance, and hazard and risk control activities.

Safety engineering makes use of lessons learned throughout the programme.

6.2 Safety requirements identification and traceability

a. Safety requirements shall be identified and traced from the system level into the design and then allocated to the lower levels.

b. When specified by the project, the identified safety requirements shall be justified in the design and presented in an appropriate document.

6.3 Safety design objectives

6.3.1 Safety policy and principles

The order of priority with respect to safety, which is part of ECSS policy, is presented in clause 4.

6.3.2 Design selection

a. Appropriate design features shall be selected to ensure inherent safety.

NOTE Such features are fail safe design solutions, damage control, containment and isolation of potential hazards.

6.3.3 Hazard reduction precedence

6.3.3.1 General

a. The following sequence of activities shall be applied to identified hazards, hazardous conditions, and functions whose failures have hazardous consequences:
   1. Hazard elimination
   2. Hazard minimization
   3. Hazard control.

6.3.3.2 Hazard elimination

a. Hazards and hazardous conditions shall, consistent with the project constraints and mission objectives, be eliminated from the design and operational concepts by the selection of design technology, architecture and operational characteristics.

6.3.3.3 Hazard minimization

a. Where hazards and hazardous conditions are not eliminated, the severity of the associated hazardous events and consequences shall, consistent with the project constraints and mission objectives, be reduced to an accepted level through the change of the design architecture, technologies, and operational characteristics allowing the substitution of those hazards by other hazards with lower potential threat.

6.3.3.4 Hazard control

6.3.3.4.1 General

a. Hazards that have not been eliminated and have been subjected to hazard minimization (as defined in 6.3.3.3a) shall be controlled through preventative or mitigation measures, associated to hazard scenarios, which are introduced into the system design and operation to avoid the events or to interrupt their propagation to consequences.

b. The following measures shall be applied in order of precedence:
   1. Design selection
   2. Automatic safety devices
   3. Warning devices
   4. Special procedures.

6.3.3.4.2 Design selection - Failure tolerance design

a. Failure tolerance is the basic safety requirement that shall be used to control most hazards.

b. The design shall tolerate a minimum number of credible failures and/or operator errors determined by the hazard consequence.

c. The supplier shall establish the list of failures to be considered as "non credible" for customer approval as early as possible in development.

6.3.3.4.3 Design selection - Design for minimum risk

a. Hazard which cannot be controlled by compliance to failure tolerance shall be reduced to an accepted level by compliance with specific safety related properties and characteristics of the design.

NOTE Examples are: structures, pressures vessels, mechanisms, material compatibility, flammability.

6.3.3.4.4 Automatic safety devices

a. Hazards that are not eliminated through design selection shall be reduced and made controllable through the use of automatic safety devices as part of the system, subsystem or equipment.

b. The safety devices, specified in 6.3.3.4.4a, shall not be dependant on human performance.

c. Use of software in automatic safety devices should be avoided.

d. If software is used in automatic safety devices, justification shall be provided.

6.3.3.4.5 Warning devices

a. When it is not practical to preclude the existence or occurrence of known hazards or to use automatic safety devices, devices shall be used for the timely detection of the condition and the generation of a warning signal.

b. This shall be coupled with emergency controls of corrective action for operators to safe or shut down the affected subsystem.

6.3.3.4.6 Special procedures

a. When it is not possible to reduce the magnitude of a hazard through the design, the use of safety devices or the use of warning devices, special procedures shall be developed to control the hazardous conditions for the enhancement of safety.

b. Special procedures shall be verified by test and appropriate training be provided for personnel.

c. Hazard detection shall be implemented if alternative means cannot be used.

d. To permit the use of real time monitoring, hazard detection and safing systems for hazard control, the availability of sufficient response time shall be verified and corresponding safing procedures be developed and verified and the personnel trained.

NOTE Special procedures are the least effective of the hazard control and risk reduction measures available. They can include emergency and contingency procedures, procedural constraints, or the application of a controlled maintenance programme.

6.3.4 Environmental compatibility

a. The system design shall meet the safety requirements under the worst-case natural and induced environments defined for the project.

b. Design and performance margins shall be established and applied for worst-case combinations of induced and natural environments and operating characteristics.

6.3.5 External services

a. Loss, malfunctioning, and sudden restoration of external services shall be defined as an input to the development phase.

b. The system design shall be defined so that catastrophic or critical consequences are not induced by loss, malfunctioning, and sudden restoration of external services.

6.3.6 Hazard detection - signalling and safing

a. Safety monitoring, display, alarm and safing capabilities shall be incorporated for manned space systems.

b. These capabilities shall provide the information to allow the crew and system operators to take actions to protect personnel from the consequences of failures within safety-critical functions and the failure of hazard control measures.

c. The system design shall provide the capability for detecting failures that result in degradation of failure tolerance with respect to the hazard detection, signalling and safing function.

d. The performance of these functions shall be verifiable during flight and ground operational phases.

e. The emergency, caution and warning function shall detect and notify the crew and system operators of emergency, warning and caution situations.

f. Safing functions and capabilities shall be included that provide for the containment or control of emergency, warning and caution situations.

g. Provisions shall be included for the monitoring of safing function execution.

h. Dedicated safing functions shall be provided for emergency situations.

i. Control of warning and caution situations shall be acceptable by system reconfiguration or by dedicated safing functions.

j. A single failure shall not cause loss of the emergency and warning function.

k. Where the operation of a safing system introduces a new hazard, inadvertent activation of the safing system shall be controlled in accordance with the failure tolerance requirements.

l. A single failure shall not cause loss of the emergency and warning functions together with the monitored functions.

m. Emergency, warning and caution data, out of limit annunciation and safing commands shall be given priority over other data processing and command functions.

n. When systems or elements are integrated into, or docked with the other systems or elements, the emergency, warning, caution, and safing function shall enable the areas of control responsibility to monitor and display the applicable parameters, and to control the related safing functions.

o. Emergency, warning, and caution parameter status information shall be available and displayed at the launch control and mission control centres in "near real time" during the operational phases.

p. It shall be possible for the crew to ascertain and monitor in "real time" the status of emergency, warning and caution parameters of non-crewed systems or elements prior to docking with crewed systems.

6.3.7 Space debris mitigation

a. The design and the operational characteristics of the space system shall be such that the generation of space debris is minimized consistent with the project constraints and mission objectives.

6.3.8 Atmospheric re-entry

a. The space vehicle shall be designed and operated (post-mission disposal manoeuvres) such that, where applicable, the risk of a catastrophic event does not exceed the level of acceptable risk specified by the project and by the launch base safety authority.

NOTE Hardware of a space system that is returned from orbit presents a potential threat to the Earth's population due to the risk of debris entering the atmosphere in an uncontrolled manner.

6.3.9 Safety of Earth return missions

a. Biological contamination (including organic-constituents) resulting from the introduction of extraterrestrial matter shall be avoided.

b. The introduction of extraterrestrial matter shall not affect the environmental conditions on Earth.

c. Extraterrestrial matter shall be treated as hazardous substances until proven otherwise.

d. A containment function for hazardous substances of the spacecraft, which prevents release in case of accidents until recovery or arrival at a dedicated containment facility, shall be provided.

e. If containment cannot be verified, the hazardous substances (and any part of the space system that has potentially been exposed) shall not be returned to Earth (unless sterilized in space).

6.3.10 Safety of human spaceflight missions

a. A mission abort capability shall be provided.

b. Safing and safe heaven functions shall be provided.

NOTE These functions can be implemented through measures such as resource conservation, increased shielding (solar flares, meteoroids and radiation), vehicle or systems reconfiguration and trajectory changes.

c. Escape and rescue functions shall be provided.

d. The capability to reconfigure the system to restore the functional capability of safety critical functions in case of failures or accidents shall be provided.

e. The capability to monitor, detect and assess hazards and effects of slow insidious events with hazardous consequences shall be detailed according to project constraints and mission objectives.

NOTE Such hazards include fatigue, corrosion, micro-organisms, aging, deterioration, contamination.

f. The space system shall provide an on-board medical facility and the capability for handling a permanently impaired or deceased crewmember.

6.3.11 Access

a. System shall be designed such that any required access to system elements during flight or ground operations can be accomplished with an accepted level of risk to personnel.

6.4 Safety risk reduction and control

6.4.1 Severity of hazardous event

a. The severity of potential consequences of identified hazardous events shall be categorized as shown in Table 6-1.

b. An understanding of the criteria defined in Table 6-1 shall be agreed between customer and supplier.

c. Detrimental environmental effects, from the point of view of severe hazardous consequences to the global public, shall be included in the consequence severity evaluation.

NOTE 1 Table 6-1 is used both in ECSS-Q-ST-30 and ECSS-Q-ST-40.

NOTE 2 This impact can be immediate and personal. It also can be on a broader scale not limited to a single person only. The hazardous consequences can be short term or long term.

NOTE 3 In space flight, the environment concerned can be outer space, including the Moon and the planets, geostationary orbit (GEO), low Earth orbit (LEO) as well as the Earth's atmosphere.

d. The availability of the following shall not be used as rationale for the reduction of the severity:

1. design features which reduce the probability of a hazardous event occurring, but which do not affect its severity;

2. warning devices, crew safe haven, or crew escape capabilities.

e. For international programmes, a coherent set of consequence severity shall be established for joint operational phases.

f. These categories shall not violate the safety policy and principles as defined in clause 4.2.1 for the protection of human life or the principles of categorization in accordance with the definition of consequence severity categories in Table 6-1.

g. The expert assessment on determining limits for exposures that do not create a hazard, those that create critical hazards and those that create catastrophic hazards shall be performed by the responsible authority, early in the design process.

NOTE Examples of responsible authority are medical boards or radiation protection committees.

h. The detailed safety requirements and measures shall be derived from allowed exposure levels.

NOTE For example: maximum allowable concentrations, maximum emission concentrations or radiation doses.

Table 6-1: Severity of consequences

Severity	Level	Dependability (refer to ECSS-Q-ST-30) *Extract from ECSS-Q-ST-30*	Safety (ECSS-Q-ST-40)
Catastrophic	1	Failures propagation	Loss of life, life-threatening or permanently disabling injury or occupational illness; Loss of system; Loss of an interfacing manned flight system; Loss of launch site facilities; Severe detrimental environmental effects.
Critical	2	Loss of mission	Temporarily disabling but not life-threatening injury, or temporary occupational illness; Major damage to interfacing flight system; Major damage to ground facilities; Major damage to public or private property; Major detrimental environmental effects.
Major	3	Major mission degradation	---
Minor or Negligible	4	Minor mission degradation or any other effect	---
NOTE: When several categories can be applied to the system or system component, the highest severity takes priority			

6.4.2 Failure tolerance requirements

6.4.2.1 Basic requirements

a. Failure tolerance shall be the basic safety requirement used to control hazards.

b. No single system failure or single operator error shall have critical or catastrophic consequences.

c. No combination of two independent system failures or operator errors shall have catastrophic consequences.

d. Safety inhibits shall be independent, verifiable, stable and stay in a safe position even in case of energy failure.

e. Multiple failures, which result from common-cause or common-mode failure mechanisms, shall be analysed as single failures for determining failure tolerance.

6.4.2.2 Redundancy separation

a. The system design shall:

1. include the capability for on-board redundancy management of safety-critical functions,
2. provide failure tolerance and redundancy status information to the flight and ground crews, including immediate crew notification in the case of failure detection, redundancy switch-over, or loss of operational redundancy,
3. include failure detection, failure isolation and switching of redundant items.

b. The capability shall be provided to the flight crew and mission control to override automatic safing and redundancy switch-over.

c. Alternate or redundant safety-critical functions shall be physically and functionally separated or protected in such a way that any event that causes the loss of one path does not result in the loss of alternative or redundant paths.

6.4.2.3 Failure propagation

a. Hardware failures or software errors shall not cause additional failures with hazardous effects or propagate to cause the hazardous operation of interfacing hardware.

6.4.3 Design for minimum risk

6.4.3.1 General

a. Technical requirements for areas of design for minimum risk shall be identified and approved by the relevant safety approval authorities

NOTE "Design for minimum risk" is a safety requirement used to control hazards by specifying safety-related properties and characteristics of the design.

6.4.3.2 Safety factors

a. Structural safety factors shall be defined and applied in accordance with ECSS-E-ST-32-10 or higher safety factor where applicable.

b. Safety margins shall be based on worst credible combinations of environmental conditions.

6.4.3.3 Fracture control

a. For manned systems, where structural failure can have catastrophic or critical consequences, structures, pressure vessels, fasteners and load-bearing paths within mechanisms shall be designed in accordance with ECSS-E-ST-32-01.

b. For unmanned systems, only pressure vessels shall be designed in accordance with ECSS-E-ST-32-01, when required by launch site safety authority.

6.4.3.4 Materials

a. Materials shall be selected and controlled in accordance with ECSS-Q-ST-70.

b. Material selection shall assure that hazards associated with material characteristics are either eliminated or controlled.

NOTE Examples of these material properties to be characterized are: toxicity, flammability, resistance to stress corrosion, outgassing, offgassing, resistance to radiation, resistance to thermal cycling, arc tracking, thermal degradation, resistance to cleaning fluid and microbiological growth.

c. If requirement 6.4.3.4b. is not feasible, the system design shall include the necessary provisions to control hazardous events associated with material characteristics in accordance with the requirements of this Standard.

NOTE An example of provisions to be included by the system design is containment of hazardous substances.

6.4.4 Probabilistic safety targets

a. When given, the probabilistic safety targets shall be used for

1. identifying and ranking major risk contributors,
2. making the acceptable risk decision for each identified hazard,
3. supporting the disposition making for those cases where nonconformance to the qualitative requirements is identified.

NOTE Probabilistic safety targets can be established by the customer for hazardous consequences at system level for each project or programme.

b. Probabilistic safety targets shall conform to the requirements given by launch safety authorities and national and international regulations.

NOTE Informative Annex E provides criteria for the establishing of probabilistic safety targets.

6.5 Identification and control of safety-critical functions

6.5.1 Identification

a. A safety critical function that, if lost or degraded, or through incorrect or inadvertent operation, can result in a catastrophic or critical hazardous consequence, shall be identified as a safety-critical function.

NOTE As an example, a series of operational events that can result in a hazard if they occur inadvertently or are operated out of order.

b. Identification shall be done without taking into account hazards controls to be or already implemented.

6.5.2 Inadvertent operation

a. Inadvertent operation of a safety-critical function shall be prevented by
   1. two independent inhibits, if it induces critical consequences, or
   2. three independent inhibits, if it induces catastrophic consequences.

6.5.3 Status information

a. The system shall provide failure tolerance and redundancy status information of safety-critical functions.

b. The system shall provide the status of at least two inhibits on functions that, if inadvertently operated, can lead to catastrophic consequences, including
   1. notification in real time in case of failure detection,
   2. announcement of any loss of operational redundancy,
   3. notification of redundancy switch-over, or
   4. changes of inhibit status.

6.5.4 Safe shutdown and failure tolerance requirements

a. The design shall either provide the capability for the safe shutdown of safety-critical functions prior to in-flight maintenance operations or conform to the failure tolerance requirements during maintenance operations.

6.5.5 Electronic, electrical, electromechanical components

a. Electronic, electrical, electromechanical (EEE) components used to support safety-critical functions in flight standard hardware shall be selected and procured in accordance with the applicable programme requirements of ECSS-Q-ST-60.

6.5.6 Software functions

6.5.6.1 Software criticality

a. Safety aspects associated with the software function shall be an integral part of the overall system safety efforts and not be assessed in isolation.

b. A software component shall be considered safety-critical if the loss or degradation of its function, or its incorrect or inadvertent operation, can result in catastrophic or critical consequences.

6.5.6.2 Analysis of safety-critical software

a. During the project life cycle, safety analysis shall be carried out to:

1. identify the criticality of software components in accordance with the severity of the consequences as defined in Table 6-1,
2. determine where and under what conditions the system can trigger hazardous events caused by the software,
3. define verification methods for hazard controls involving software,
4. provide verification evidence of hazard control implementation.

6.5.6.3 Evaluation of software criticality

a. The criticality of a software component shall be evaluated taking into account the overall system design which can provide for, e.g. back-up or emergency procedures, hardware inhibits and certain time to effect.

6.5.6.4 Software development

a. A safety-critical software component shall be designed, implemented, verified and operated according to the engineering and product assurance requirements defined in ECSS-E-ST-40 and ECSS-Q-ST-80.

b. Safety-critical software shall be analysed for the identification and verification of adequate software controls and inhibits and validated accordingly.

c. The level of required software product assurance effort shall be determined in accordance with the criticality of the software component.

6.6 Operational Safety

6.6.1 Basic requirements

a. Safety involvement in the operational phase shall be planned.

b. Responsibilities, rules and contingency procedures shall be established prior to operation for hazardous “limit” conditions that can occur during ground and in-flight operations.

c. Operating ranges and performance limits for safe operation shall be established and specified.

d. The design shall not require continuous active control by personnel in order to stay within the established operating ranges and performance limits.

e. Man-machine interfaces shall be designed and the personnel tasks shall be scoped to reduce the potential for hazardous events resulting from human error to an accepted level.

f. Limits for crew exposure to natural and system-induced environments shall be established and maintained by design features or operational constraints that cover nominal, contingency, and emergency operational modes, in order to preclude crew injury or inability to perform safety-critical functions.

6.6.2 Flight operations and mission control

6.6.2.1 Launcher operations

a. Hazards to the humans, public and private property and the environment, resulting from launcher system operation or malfunction shall be precluded by compliance with the regulations of the launch safety authority.

6.6.2.2 Contamination

a. Normal or abort operations shall not result in contamination of the Earth's environment that endangers human health, crops or natural resources or that exceed limits set by national or international regulations.

6.6.2.3 Flight rules

a. Flight rules shall be prepared for each mission that outline pre-planned decisions in case of off-nominal situations and consistent with safety requirements.

6.6.2.4 Hazardous commanding control

a. Hazardous commanding control shall ensure that all hazardous commands are identified.

b. Hazardous commanding control shall ensure that failure modes, associated with flight and ground operation - including hardware, software and procedures - used in commanding from control centres or other ground equipment, are included in the safety assessment.

c. Hazardous commanding control shall ensure that the system design provides protection to avoid the erroneous acceptance of commands that can result in catastrophic or critical consequences.

d. .Hazardous commanding control shall ensure that commands, which can result in catastrophic or critical hazardous consequences, are not performed until they are authorized and verified.

6.6.2.5 Mission operation change control

a. Mission operation change control shall ensure that all changes, which are desired or become necessary during mission, are reviewed for safety impact.

b. Mission operation change control shall ensure that the responsible safety approval authority approves all operational change requests with safety impact.

6.6.2.6 Safety surveillance and anomaly control

a. Safety status parameters shall be identified.

b. Safety status parameters shall be monitored.

c. Deviation from specified limits shall be managed.

6.6.2.7 Hazardous debris, fallout and impact control

a. In the case of a deviation from the planned launch trajectory during ascent, launch vehicle stages shall be remotely destroyed or have their propulsion engines shut off to prevent stages or debris from falling outside pre-defined safe areas.

b. The launch vehicle and spent stage trajectories shall be monitored to determine vehicle, stage or debris impact points.

c. Residual propellants contained in spent or aborted suborbital stages shall be safely dispersed.

6.6.3 Ground operations

6.6.3.1 Applicability

a. Safety requirements of the clause shall be applied during the following ground operations:

1. development, qualification or acceptance testing;
2. assembly, integration or test operations;
3. launch site operations;
4. servicing or turn-around operations; and
5. transportation or handling operations,

6.6.3.2 Initiation

a. The supplier shall establish procedures to perform safety readiness reviews and inspections prior to the performance of any applicable operation.

6.6.3.3 Review and inspection

a. To verify conformance to safety requirements, readiness reviews and inspections shall include safety review and assessment of facilities, equipment (incl. GSE), test articles, operating, test and contingency procedures, access controls, and personnel capabilities to comply with the safety requirements.

6.6.3.4 Hazardous operations

a. Hazardous operations shall be monitored for conforming to safety requirements and procedures, and for the possible development of unforeseen hazardous situations.

b. Where necessary, contingency and emergency plans or procedures shall be established and verified prior to the commencement of the operation.

c. The safety manager or safety relevant authority shall have the authority to stop any operation that does not conform to safety requirements.

6.6.3.5 Launch and landing site

a. Launch, landing, turn-around and mission operations shall be subject to hazard analysis.

b. For ground operations, the analysis shall address the:

   1. potential hazardous consequences of human error and procedural deficiencies;

   2. adequacy and maintenance of operational margins;

   3. potential for human exposure to hazards and hazardous effects;

   4. requirements for operator and flight crew training;

   5. adequacy of information and data provided by the flight hardware, ground support equipment (GSE), or test equipment, as appropriate, to support the performance of the operations in accordance with all applicable safety requirements (including all safety regulations).

6.6.3.6 Ground support equipment

a. All Ground support equipment (GSE) shall be subjected to hazard analysis.

b. All GSE shall conform to the 'Essential Health & Safety Requirements' of all applicable EU 'New Approach directives'.

c. Conformance to 6.6.3.6b. shall be shown by the addition of the 'CE' mark to the product and the issuing of a 'Declaration of Conformity'.

d. Conformance to any other product related directives shall be demonstrated.

NOTE Further guidance is given in Annex G.

7
Safety analysis requirements and techniques

7.1 Overview

Safety risks are the result of the hazardous characteristics associated with the:

- design, including the technology selected, the physical arrangement of elements, subsystems and equipment, and software functions;
- operating modes;
- potential for operator error;
- operating environment;
- hazardous effects that result from the failure of functions (including software).

7.2 General

a. Safety analysis shall be performed in a systematic manner as a basis for all applicable phases and to ensure that hazards are identified, eliminated or minimized and controlled and safety risks are assessed and reduced.

b. Safety analyses shall be initiated early in the design process and provide concurrent support to project engineering in the selection of the least hazardous design and operational options that are compatible with the project mission and programme constraints and conform to the requirements.

c. The results of safety analyses shall also be used to support project management in the assessment of the overall risks, verification of risk reduction, ranking of risk sources, support to project resource allocation, monitoring of risk trends, and residual risk acceptance.

d. Analysis shall always be made with reference to a defined configuration baseline as defined by ECSS-M-ST-40.

7.3 Assessment and allocation of requirements

7.3.1 Safety requirements

a. The supplier shall respond to and comply with the applicable safety requirements for the project.

7.3.2 Additional safety requirements

a. The supplier shall identify additional safety requirements, where applicable, through the use of lessons learned from previous projects and the safety analyses performed during the project.

7.3.3 Define safety requirements - functions

a. The supplier shall define the safety requirements for the various functions of the system.

7.3.4 Define safety requirements - subsystems

a. The supplier shall define the safety requirements associated with the various subsystems and lower levels.

7.3.5 Justification

a. The supplier shall justify to the customer the proposed allocation of safety requirements at the latest at the end of the detailed definition phase.

7.3.6 Functional and subsystem specification

a. The supplier shall ensure that the function and subsystem safety requirements are included in the relevant functional and subsystem specification.

7.4 Safety analyses during the project life cycle

a. Safety analysis shall be refined and updated in an iterative manner as the design process proceeds, to ensure that hazards and hazardous events are assessed, and that the relevant detailed design and operational requirements, hazard controls, and verification activities are defined and implemented.

NOTE Refer to 5.7 for detailed safety programme tasks in the different project phases

7.5 Safety analyses

7.5.1 General

a. The safety analysis report shall be established in conformance with the DRD in Annex D in order to gather results of safety analyses, which use deterministic and probabilistic methods which are described in the clauses 7.5.2 to 7.5.4.

7.5.2 Hazard analysis

a. Hazard analysis shall be performed in a systematic manner, beginning in the concept phase and continuing through the operational phase, including end-of-life and disposal.

b. Hazard analysis shall support the hazard reduction process.

c. Hazard analysis shall identify and evaluate:

   1. hazards associated with system design, its operation (both on ground and in flight) and the operation environment;
   2. the hazardous effects resulting from the physical and functional propagation of initiator events;
   3. the hazardous events resulting from the failure of system functions and functional components;
   4. time critical situations.

d. The following potential initiator events shall be considered:

   1. hardware failure (random or time dependent);
   2. latent software error;
   3. operator error;
   4. design inadequacies, including:
      (a) inadequate margins;
      (b) unintended operating modes caused by sneak-circuits;
      (c) material inadequacies and incompatibilities;
      (d) hardware-software interactions;
   5. natural and induced environmental effects;
   6. procedural deficiencies.

e. Hazard analysis includes a systematic analysis of the "system" operations and operating procedures that shall be performed in the detailed design and operational stages of a project.

   NOTE This analysis evaluates the capability of the system to be operated safely, to determine the safest operating modes, and to evaluate the acceptability of the operating procedures.

f. The systematic analysis of system operation and operating procedures shall be repeated as the design and operational detail evolves, including the system's operational modes and man-machine interfaces.

7.5.3 Safety risk assessment

a. Safety risk assessment shall

1. comprise the identification, classification and ranking of safety risks and their contributors,
2. be based on deterministic hazard analysis by combining the consequence severity and the likelihood of occurrence of the consequence,
3. be used to facilitate effective and efficient safety risk reduction and control,
4. support project risk management as defined in ECSS-M-ST-80,
5. assess compliance with probabilistic safety targets.

NOTE 1 The estimation of event likelihoods is based on the use of different sources of data i.e.:

- previous experience on the particular system (i.e. measured or observed directly relevant test or experience data),
- data from other systems or projects (i.e. extrapolation from generic data, similarity data, or physical models), and
- expert judgment (i.e. direct estimation of likelihoods by domain specialists).

NOTE 2 The determination of likelihood is not a mean to downgrade the severity of function (see 6.4.1d)

b. Safety risk assessment shall be started early in the design process and performed in progressive steps during the implementation of the safety programme.

7.5.4 Supporting assessment and analysis

7.5.4.1 General

a. Following supporting assessment and analysis methods shall be used as necessary (tailored by project) to support hazards analysis and safety risk assessment.

NOTE 1 Example of tailoring by project is when the supporting assessment and analysis methods are not applicable in e.g. unmanned missions.

NOTE 2 Assessments and analyses from ECSS-Q-ST-30 can be used to support safety assessment.

b. Supporting analyses shall be agreed with all relevant parties.

7.5.4.2 Warning time analysis

a. Warning time analysis shall be performed during the concept definition phase and the design and development phase in order to evaluate time-critical situations identified in the hazard analysis and to support the implementation of hazardous-situation detection and warning devices or contingency procedures.

b. The analysis shall determine the

   1. time interval during which the event is detected and the response action taken;

   2. detection capability of the proposed design with respect to detection sensitivity and detection time;

   3. resultant time available for response;

   4. adequacy of the proposed design or contingency procedures, including emergency evacuation, rescue, system reconfiguration, redundancy switching, and maintenance.

c. The detection times shall be determined from the

   1. occurrence of the initiating event to the time when a hazardous consequence occurs (propagation time);

   2. occurrence of the initiating event to the time of earliest detection or annunciation; and

   3. time taken for corrective action to be implemented.

7.5.4.3 Caution and warning analysis

a. Caution and warning analysis shall be performed during the concept definition phase and the design and development phase of human space flight programmes in order to identify

   1. emergency, warning, and caution parameters;

   2. the required safing functions and capabilities;

   3. limit sensing requirements;

   4. the applicability of the individual "caution and warning" functions to the different mission phases.

b. The caution and warning analysis shall utilize the results of the warning time and hazards analyses as appropriate.

7.5.4.4 Common-cause and common-mode failure analysis

7.5.4.4.1 Multiple failures

a. Multiple failures, which result from common-cause or common-mode failure mechanisms, shall be analysed as single failures for determining failure tolerance.

7.5.4.4.2 Identification of requirements and scope

a. The supplier shall identify the requirement for and the scope of dedicated common-cause and common-mode analyses by means of the review of the results of the other safety analyses, such as FTA and hazard analysis, and of the characteristic of the system and of its environment.

7.5.4.4.3 Identification of common-cause failures

a. The supplier shall identify potential common-cause failures by assessment of the effects of common-causes.

NOTE For example: radiation, thermal environment and fires.

b. The common-cause failure analysis shall be performed in coordination with the FTA and the hazard analysis.

NOTE The analysis of common-cause failures can require that use be made of the result of dedicated engineering analyses, e.g. thermal analyses, meteorite or debris impact analysis.

7.5.4.4.4 Analysis of common-mode failures

a. Common-mode failures shall be analysed by means of the use of check-lists (to be established by the supplier) that list potential common-modes for system components during the manufacturing, integration, test, operation and maintenance phases.

b. The common-mode analysis shall be coordinated with the FMEA/FMECA.

7.5.4.4.5 Integration of results

a. Results of common-cause and common-mode analysis shall be integrated with the results of the system level safety analyses (fault tree analysis, hazard analysis).

7.5.4.5 Fault tree analysis

a. The fault tree analysis shall be used to establish the systematic link between the system-level hazard and the contributing hazardous events and subsystem, equipment or piece part failure.

b. A fault tree analysis, or its equivalent, shall be performed to verify the failure tolerance requirements.

NOTE Refer to ECSS-Q-ST-40-12 “Fault tree analysis - Adoption notice ECSS/IEC 61025” for further instructions on fault tree analyses.

7.5.4.6 Human error analysis

a. Whenever safety analyses identify operator errors as a cause of catastrophic or critical hazards, a dedicated analysis shall be carried out.

b. The human error analysis shall be used to support the safety analysis for the identification of human operator error modes and their effects and for the definition of adequate countermeasures to prevent or control human operator errors.

c. The human error analysis shall be developed from the early phases of the project onwards in order to define recommendations for the hardware and software design, procedure development and training preparation programme.

7.5.4.7 Failure modes, effects and criticality analysis

a. The results of failure modes and effects analysis (FMEA) or failure modes, effects and criticality analysis (FMECA) shall be used to support the hazard analysis in the evaluation of the effects of failures. FMEA/FMECA and hazard analysis are complementary analyses.

NOTE Refer to ECSS-Q-ST-30-02 for further instructions on FMEA/FMECA.

7.5.4.8 Zonal analysis

a. Zonal analysis shall be performed where redundancy is used to reduce the probability of losing a function or of inadvertently actuating a safety-critical function.

b. The objectives of the zonal analysis shall ensure that equipment installation meets the adequate safety requirements regarding:

1. basic installation rules and space practices;
2. interaction between subsystems;
3. implication of operator errors;
4. effects of external events.

NOTE Zonal analysis is the systematic inspection of the topology of a system, the evaluation of potential component-to-component interactions with and without failure, and the assessment of the severity of potential hazards inherent in the system installation.

8
Safety verification

8.1 General

a. A system shall be in place that tracks all hazards and related risks, to relate all verifications of the corresponding hazard uniquely to unambiguous causes and controls.

b. For common techniques for verification of design features used to control hazards, the requirements of ECSS-E-ST-10 shall apply.

c. To successfully complete the safety process, positive feedback shall be provided on completion results for all verification items associated with a given hazard.

8.2 Hazard reporting and review

8.2.1 Hazard reporting system

a. The supplier shall establish a hazard reporting system for tracking the status of all identified hazards.

b. The system shall be applied for all hazards with potentially catastrophic or critical consequences.

c. The supplier shall report, and provide evidence, that
   1. controls are defined and agreed;
   2. verification methods are defined and agreed;
   3. verification is completed.

d. If verification cannot be completed, the supplier shall establish a Safety Verification Tracking Log (SVTL) (refer to clause 8.5.1a.).

8.2.2 Safety status review

a. Status of hazard control and risk reduction activities shall be reviewed at safety progress meetings and project safety reviews for compliance with decisions taken and achievement of intended results.

8.2.3 Documentation

a. All hazard documentation shall be formally issued for each safety review and major project review, as specified in clause 5.11).

8.3 Safety verification methods

8.3.1 Verification engineering and planning

a. Verification engineering shall select the verification methods consistent:

   1. with the verification requirements documented in the hazard report,

   2. with the launch base safety rules.

b. Verification planning shall commence in an integrated manner upon selection of the control method.

8.3.2 Methods and reports

a. Safety verification methods shall include alternatively or in combination review of design, analysis, inspection and test.

b. For all safety verifications traceability shall be provided.

8.3.3 Analysis

a. All relevant technical safety and engineering analyses performed or updated with analysis in respect to the as-built configuration shall be used for verification.

b. When similarity analysis is provided, for tracking purposes it shall contain a copy of (or a unique reference to) the referenced previous verification, verification procedure and requirement valid at the time of the first verification.

8.3.4 Inspections

8.3.4.1 General

a. Inspections which are considered as necessary in order to meet safety requirements of the system shall be identified and included in user manuals and procedures.

8.3.4.2 Preflight inspections

a. All preflight safety inspections shall be assessed for inclusion in the MIP list.

NOTE If preflight safety inspections are included on the MIP list, closeout is feasible by MIP reporting or individual reporting as appropriate.

b. Launch preparation inspections shall be entered into the launch base procedure.

c. The closeout shall be given by the approved launch authority procedure.

d. Late access procedures shall be the subject of training and be performed by qualified personnel.

e. Training for flight crew and mission operation teams shall be performed, including specific safety briefing, training and mission simulation.

f. Close-out shall be by safety-approved procedure, documented training session and simulations.

8.3.4.3 Inflight inspections

a. Inflight inspections shall be entered into flight procedures and operation manuals.

8.3.5 Verification and approval

a. The supplier shall select, and propose to the safety approval authority, the safety verification methods to be used in conformance to the applicable safety requirements.

b. The results of safety verification shall be submitted for approval to the relevant safety approval authority.

8.4 Verification of safety-critical functions

8.4.1 Validation

a. Safety-critical functions shall be verified by testing which include application of the operating procedures, the "man-in-the-loop", and the verification of the effectiveness of applicable failure tolerance requirements.

b. The tests shall include the demonstration of nominal, contingency and emergency operational modes.

8.4.2 Qualification

a. The safety-critical characteristics of all safety-critical functions shall be qualified by test.

b. Safety-critical function qualification testing shall include the determination of performance margins considering worst case combinations of induced and natural environments and operating conditions.

c. Qualification "by similarity" shall not be applied except after customer approval on a case-by-case basis.

8.4.3 Failure tests

a. Induced failure tests shall be performed when required by safety analysis for evaluating failure effects, and for demonstrating failure tolerance conformance in safety-critical functions.

8.4.4 Verification of design or operational characteristics

a. Verification of unique safety required design or operational characteristics shall form part of the development, qualification or acceptance testing programmes as appropriate.

8.4.5 Safety verification testing

a. Where full-scale testing is not performed, equivalent safety verification method based on technically representative hardware or models shall be justified, approved and performed.

b. For the verification of hazard controls in catastrophic hazards where non-flight equipment replaces part of the flight equipment to test a flight function the verification shall be performed independently by a third party which was not involved in the design and qualification of the flight model (FM).

8.5 Hazard close-out

8.5.1 Safety assurance verification

a. A safety verification tracking log (SVTL) shall be established, in conformance with the DRD in Annex C, to collect all the open verification items of the different hazard reports from the safety analysis.

b. In time for acceptance by the customer, and in preparation of transfer to the next stage of system integration, the safety manager shall verify that:

   1. hazard close-outs performed so far by the responsible engineer are still valid;

   2. the verifications reflect the as-built or as-modified status of the hardware;

   3. all open verifications at this time are acceptable for transfer to the next stage of system integration;

   4. all open verifications are entered into the verification tracking log (SVTL);

   5. the verification tracking log is maintained to reflect the current status.

c. If the safety verification constrains any ground operations, the safety manager shall give notification to the safety review panel.

8.5.2 Hazard close-out verification

a. The safety manager shall assure that each hazard considered for closure has the approval by the safety approval authority, verifying that

1. hazards not eliminated are controlled in accordance with the applicable requirements and associated verification activities are successfully completed, or, when applicable,

2. deviations from, or waivers of requirements, are granted by the safety approval authority.

8.6 Declaration of conformity of ground equipment

a. All ground equipment that falls into the scope of an applicable 'New Approach directive' shall be 'CE' marked and supplied with a supporting 'Declaration of Conformity' and User Manual detailing all safety warnings."

NOTE Additional information is provided in Informative Annex G.

Annex A (informative)
Analyses applicability matrix

Scope of the Table A-1 is to present relation of documents associated to safety activities to support project review objectives as specified in ECSS-M-ST-10.

NOTE This table constitutes a first indication for the data package content at various reviews. The full content of such data package is established as part of the business agreement, which also defines the delivery of the document between reviews.

The table lists the documents necessary for the project reviews (identified by "X").

The various crosses in a row indicate the increased levels of maturity progressively expected versus reviews. The last cross in a row indicates that at that review the document is expected to be completed and finalized.

NOTE All documents, even when not marked as deliverables in Table A-1, are expected to be available and maintained under configuration management as per ECSS-M-ST-40 (e.g. to allow for backtracking in case of changes).

Documents listed in Table A-1 are either ECSS-Q-ST-40 DRDs, or DRDs to other ECSS-Q-40-XX standards.

Table A-1: Safety DRL

Document or DRD title	Phase												Document or DRD reference
	A	B		C	D		E					F	
	PRR	SRR	PDR	CDR	QR	AR	ORR	FRR	LRR	CRR	ELR	MCR	
Safety programme plan	X	X	X	X	X	X	X	X	X	X			ECSS-Q-ST-40 Annex B
Safety verification tracking log					X	X							ECSS-Q-ST-40 Annex C
Safety analysis report (including hazard reports)		X	X	X	X	X	X	X	X	X		X	ECSS-Q-ST-40 Annex D
Fault tree analysis				X	X	X							ECSS-Q-ST-40-12

Annex B (normative)
Safety programme plan - DRD

B.1 DRD identification

B.1.1 Requirement identification and source document

This DRD is called from ECSS-Q-ST-40, requirement 5.2a.

B.1.2 Purpose and objective

The plan defines:

- the safety programme tasks to be implemented;
- the personnel or supplier responsible for the execution of the tasks;
- the schedule of safety programme tasks related to project milestones;
- safety programme activity interface with project engineering and with other product assurance activities;
- how the supplier accomplishes the tasks and verifies satisfactory completion (by reference to internal procedures as appropriate).

B.2 Expected response

B.2.1 Contents

<1> Description

a. The safety programme plan shall include a description of the project safety organization, responsibilities, and its working relationship and interfaces with product assurance disciplines (reliability, maintainability, software product assurance, parts, materials and processes and quality assurance according to ECSS-Q-ST-10, -20, -30, -60, -70 and -80), with configuration management according to ECSS-M-ST-40, system engineering according to ECSS-E-ST-10, design and other project functions and departments of organizations.

b. The safety programme plan shall describe how the provisions of ECSS-Q-ST-40 are implemented:

1. Safety programme and organization;
2. Safety engineering;
3. Safety analysis requirements and techniques;
4. Safety verification;
5. Operational safety.

<2> Safety and project engineering activities

a. The plan shall show how the project safety organization implements concurrent safety and project engineering activities in continuous support of the project design and development process.

<3> Supplier and lower tier supplier premises

a. The plan shall describe how safety-related activities and requirements are defined for and controlled at suppliers' and lower tier suppliers' premises.

<4> Conformance

a. The plan shall make provisions for assuring conformance to safety requirements and regulations that are applicable to any other facilities and service that are utilized during the course of the project.

B.2.2 Special remarks

a. The safety programme plan may be incorporated within the Product Assurance Plan when agreed between the relevant parties.

Annex C (normative)
Safety verification tracking log (SVTL) DRD

C.1 DRD identification

C.1.1 Requirement identification and source document

This DRD is called from ECSS-Q-ST-40, requirement 8.5.1a.

C.1.2 Purpose and objective

As part of the Safety Data Package (SDP), a SVTL log collects all the open safety verification items from the different safety analysis/hazard reports of the SDP at the end of the production and qualification phase of the project. It provides information of the verification effort and gives reference to the close out documents (e.g. test reports, analyses, and procedures). Depending on the number and severity of the open verification items it can be the basis for the decision to put the next processing steps (like acceptance or integration into the next higher level) into hold.

The SVTL is based on:

- inputs from the different safety verification tasks i.e. hardware and software changes, tests, review of design activities, analyses, inspections and development of procedures which are performed as agreed per "hazard reports" of the Flight-SDP (FSDP) and the Ground-SDP (GSDP) - or a combination thereof,
- other information like constraints and schedule.

NOTE An example of a format that can be used for the SVTL is presented in Figure C-1.

C.2 Expected response

C.2.1 Contents

<1> General information

a. The SVTL shall identify the following general information:

1. name of the project for which it has been established;

2. project documentation identification number;
3. applicability for flight or ground safety verifications;
4. indication of the specific page number followed by the total number of pages;
5. name of the equipment, payload or experiment for which the SVTL has been established;
6. mission or flight to which the equipment, payload or experiment has been manifested;
7. dates of issue and update.

<2> Log number

a. For each verification item to be tracked a unique identifier shall be used.

b. The SVTL shall use the designations assigned by the safety manager.

<3> Hazard report number

a. The identification number of the hazard report containing the verification item shall be indicated.

<4> Safety verification number

a. The verification method or the verification means shall be transferred from the hazard report including the procedures by number and title.

<5> Ground operations constrained

a. The input of “yes” or “no” shall indicate whether this safety verification constrains any ground operations.

b. If “yes” for flight tracking log: an attachment shall be provided that identifies which ground operation is constrained.

c. If “yes” for ground tracking log: the ground operation constrained by this verification shall be indicated specifically in the user manual and included as a step in a procedure.

<6> Independent verification required, "yes" or "no"

a. The input of "yes" or "no" shall indicate whether the verification has to be performed independently (in accordance with 8.4.5b).

<7> Scheduled completion date

a. The planned date for the completion of the verification shall be indicated.

<8> Method of closure/comments

a. The SVTL log shall indicate the title and serial number of the tests, review of designs, inspections and analyses by which this verification is formally closed.

b. Any appropriate information or remarks may be added.

C.2.2 Special remarks

The SVTL is part of the SDP at the end of the qualification phase.

Safety verification tracking log		Flight ❑	Ground ❑	page ___ of ___	
Project ID:					
Equipment, payload, mission				Issue date	updated

Log no.	Hazard report number	Safety verification number	Safety verification method (Identify procedures by number and title)	Ground operations constrained	Independent verification required	Scheduled completion date	Completion date	Method of closure/comments (Provide reference ID)

Figure C-1: Safety verification tracking log (SVTL)

Annex D (normative) Safety analysis report including hazard reports - DRD

D.1 DRD identification

D.1.1 Requirement identification and source document

This DRD is called from ECSS-Q-ST-40, requirement 7.5.1a.

D.1.2 Purpose and objective

The safety analysis report documents the results of safety analysis. The safety analysis report contains a set of hazard reports, which documents the results of the systematic identification, evaluation, reduction, verification and tracking of hazards.

D.2 Expected response

D.2.1 Contents

<1> Safety analysis report preliminary elements

a. Title - The title of the safety analysis report shall identify the applicable project.

b. Title page - A title page shall be provided.

c. Contents - A contents list shall be provided.

d. Foreword - A foreword shall be provided.

e. Introduction - An introduction shall be provided.

<2> Safety analysis report content

a. The safety analysis report shall identify the following general information:

1. the project documentation identification number, the title of the safety analysis report, date of release and release authority;
2. the project phase;
3. identification of which organizational entity prepared the document;

4. information regarding the approval of the document;
5. a statement of effectivity identifying which other documents have been cancelled and replaced in whole or in part.

b. The safety analysis report shall contain the following analysis specific information:
   1. objective of safety analysis;
   2. applicable requirements relevant to the safety analysis;
   3. description of system design & operation from a safety point of view;
   4. description of safety analysis process and methods;
   5. detailed results of safety analysis documented in form of a set of hazard reports (see D.2.1<2>c.);
   6. list of safety critical functions;
   7. safety critical item list;
   8. safety input to risk management;
   9. support analyses used (e.g. FTA, FMEA/FMECA);
   10. overall conclusions from safety assessment.

c. Each hazard report shall contain as a minimum the following data:
   1. title;
   2. types of hazards and description of their manifestation in the system design and operational configuration and environment;
   3. identified hazard scenario with description of causes (associated with the hazard manifestation), hazardous events (physical and functional propagation) and consequences;
   4. consequence severity category;
   5. propagation time from cause to consequence;
   6. likelihood of hazard scenario and magnitude of safety risk (optional);
   7. applicable safety requirements;
   8. hazard reduction measures (implementation of safety requirements, hazard elimination or minimization and control);
   9. verification measures;
   10. safety risk trend after hazard reduction (optional);
   11. status (safety verification actions open or closed, non-conformances and waivers);
   12. approval;
   13. acceptance of safety risk (optional).

   NOTE Example of formats that can be used for "Hazard and safety risk register", and "Ranked hazard and safety risk log" are given in the annexes of ECSS-Q-ST-40-02.

D.2.2 Special remarks

The safety analysis reports form part of the safety data package.

Annex E (informative)
Criteria for probabilistic safety targets

E.1 Objectives of probabilistic safety targets

a. Probabilistic safety targets can be established by the customer for hazardous consequences at system level for each project or programme.

b. When given, these probabilistic targets should be used for:

   1. identifying and ranking major risk contributors,

   2. making the acceptable risk decision for each identified hazard,

   3. supporting the disposition making for those cases where nonconformance to the qualitative requirements is identified.

E.2 Criteria for probabilistic safety targets

a. Probabilistic safety targets should conform to the requirements given by launch safety authorities and national and international regulations.

b. With respect to safety targets for the ground and flight personnel, the individual risk should not exceed that accepted for other professionally and comparably exposed personnel.

   NOTE E.g. risk for crew members should not exceed that for test pilots, risk for ground personnel should not exceed that for similarly exposed industrial workers.

c. With respect to safety targets for the civil population, the total risk for the exposed ground population should not exceed that caused by other hazardous human activities.

   NOTE E.g. risk from overflight of commercial aircraft or chemical plants.

d. The detailed project requirements on the acceptable level of risk should be defined in the project risk management policy according to ECSS-M-ST-80 and considered in the tailoring of the project specific safety requirements.

Annex F (informative) Applicability guidelines

This matrix determines the applicability of ECSS-Q-ST-40 to the different space systems, i.e.:

- *Satellite:* Un-manned payload on an expendable launch vehicle,
- *Un-manned safety-critical system:* Un-manned space system (comprising the flight segment and the ground segment) including or providing functions which are safety critical,
- *Manned space system:* Manned space system (comprising the flight segment and the ground segment),
- *Launch vehicle:* Vehicle designed to carry payloads into space.

Tailoring of the requirements identified as applicable (or partially applicable) is necessary for taking into account the specific requirements for, or the peculiar characteristics of, the system.

Clause	Headline	Un-manned space system		Manned space system	Launch vehicle		Remarks
		Satellite	Safety critical systems		for un-manned space-craft	for manned space-craft	
5	**Safety programme**						
5.1	Scope	Y	Y	Y	Y	Y	
5.2	Safety programme plan	Y	Y	Y	Y	Y	
5.3	Conformance	Y	Y	Y	Y	Y	
5.4	Safety organization						
5.4.1	Safety manager	Y	Y	Y	Y	Y	
5.4.2	Safety manager access and authority						
5.4.2.1	Access	Y	Y	Y	Y	Y	
5.4.2.2	Authority	Y	Y	Y	Y	Y	
5.4.3	Safety audits	Y	Y	Y	Y	Y	
5.4.4	Approval of documentation	Y	Y	Y	Y	Y	
5.4.5	Approval of hazardous operations	Y	Y	Y	Y	Y	
5.4.6	Representation on boards	Y	Y	Y	Y	Y	
5.4.7	Safety approval authority	Y	Y	Y	P/A [1]	Y	[1]) according to safety launcher authority

Clause	Headline	Un-manned space system		Manned space system	Launch vehicle		Remarks
		Satellite	Safety critical systems		for un-manned space-craft	for manned space-craft	
5.5	Safety risk assessment and control	P/A [3]	Y [2]	Y [2]	P/A [2]	Y [2]	[2]) Use of *probabilistic* safety risk assessment subject to specific project requirements [3]) Use of *probabilistic* safety risk assessment if required by inter-national rules (e.g., nuclear material onboard)
5.6	Safety critical items	Y	Y	Y	Y	Y	
5.7	Project phases and safety review cycle						
5.7.1	Safety program tasks and reviews	P/A[4]	Y	Y	P/A[4]	P/A[4]	[4])As appropriate for the project
5.7.1.1	Mission analysis / Needs identification - Phase 0	P/A[4]	Y	Y	P/A[4]	P/A[4]	[4])As appropriate for the project
5.7.1.2	Feasibility - Phase A	P/A[4]	Y	Y	P/A[4]	P/A[4]	[4])As appropriate for the project
5.7.1.3	Preliminary definition - Phase B	P/A[4]	Y	Y	P/A[4]	P/A[4]	[4])As appropriate for the project
5.7.1.4	Detailed definition, production and qualification testing - Phase C/D	P/A[4]	Y	Y	P/A[4]	P/A[4]	[4])As appropriate for the project
5.7.1.5	Utilization - Phase E	P/A[4]	Y	Y	P/A[4]	P/A[4]	[4])As appropriate for the project
5.7.1.6	Disposal - Phase F	P/A[4]	Y	Y	P/A[4]	P/A[4]	[4])As appropriate for the project
5.7.2	Progress meeting	Y	Y	Y	Y	Y	
5.7.3	Safety reviews	Y	Y	Y	Y	Y	As appropriate for the project
5.8	Safety compliance demonstration	Y	Y	Y	Y	Y	
5.9	Safety training						
5.9.1	General	Y	Y	Y	Y	Y	
5.9.2	Product specific training	Y	Y	Y	Y	Y	
5.9.3	General awareness briefing	Y	Y	Y	Y	Y	
5.9.4	Basic technical training	Y	Y	Y	Y	Y	
5.9.5	Training records	Y	Y	Y	Y	Y	
5.10	Accident-incident reporting and investigation	Y	Y	Y	Y	Y	
5.11	Safety documentation						
5.11.1	General	Y	Y	Y	Y	Y	
5.11.2	Safety data package	Y	Y	Y	P/A[5]	Y	[5]) According to the launch base safety rules, if any
5.11.3	Safety deviations and waivers						
5.11.3.1	Request for deviation or waiver	Y	Y	Y	P/A[6]	Y	[6]) Following the process defined by the Safety launch base rules, if any, and specific protocol

Clause	Headline	Un-manned space system		Manned space system	Launch vehicle		Remarks
		Satellite	Safety critical systems		for un-manned space-craft	for manned space-craft	
							applicable. Only waivers for launchers
5.11.3.2	Assessment of deviation or waiver	Y	Y	Y	Y	Y	
5.11.3.3	Acceptance by the safety approval authority	Y	Y	Y	Y	Y	
5.11.3.4	Review and disposition	Y	Y	Y	Y	Y	
5.11.4	Safety lessons learned	Y	Y	Y	Y	Y	
5.11.5	Documentation of safety critical items	Y	Y	Y	Y	Y	
6	**Safety engineering**						
6.1	Overview	Non-normative					
6.2	Safety requirements identification and traceability	Y	Y	Y	Y	Y	
6.3	Safety design objectives						
6.3.1	Safety policy and principles	Y	Y	Y	Y	Y	
6.3.2	Design selection	Y	Y	Y	Y	Y	
6.3.3	Hazard reduction precedence						
6.3.3.1	General	Y	Y	Y	Y	Y	
6.3.3.2	Hazard elimination	Y	Y	Y	Y	Y	
6.3.3.3	Hazard minimization	Y	Y	Y	Y	Y	
6.3.3.4	Hazard control	Y	Y	Y	Y	Y	
6.3.4	Environmental compatibility	Y	Y	Y	Y	Y	
6.3.5	External services	Y	Y	Y	Y	Y	
6.3.6	Hazard detection - signalling and safing	N/A	P/A [7]	Y	N/A	Y	[7]) as appropriate for the project
6.3.7	Space debris mitigation	Y	Y	Y	Y	Y	
6.3.8	Atmospheric re-entry	Y	Y	Y	Y	Y	
6.3.9	Safety of Earth return missions	Y	N/A	Y	Y	Y	
6.3.10	Safety of human spaceflight missions	N/A	N/A	Y	N/A	Y	
6.3.11	Access	Y	Y	Y	Y	Y	
6.4	Safety risks reduction and control						
6.4.1	Severity of hazardous event	Y	Y	Y	Y	Y	
6.4.2	Failure tolerance requirements						
6.4.2.1	Basic requirements	Y	Y	Y	Y	Y	
6.4.2.2	Redundancy separation	N/A	Y	Y	N/A	Y	
6.4.2.3	Failure propagation	Y	Y	Y	Y	Y	
6.4.3	Design for minimum risk						
6.4.3.1	General	Y	Y	Y	Y	Y	
6.4.3.2	Safety factors	Y	Y	Y	Y	Y	
6.4.3.3	Fracture control	Y	Y	Y	Y	Y	
6.4.3.4	Materials	Y	Y	Y	Y	Y	
6.4.4	Probabilistic safety targets	N/A	P/A	P/A	P/A	P/A	Applicability of probabilistic safety targets to be defined by the project

Clause	Headline	Un-manned space system		Manned space system	Launch vehicle		Remarks
		Satellite	Safety critical systems		for un-manned space-craft	for manned space-craft	
6.5	Identification and control of safety-critical functions						
6.5.1	Identification	Y	Y	Y	Y	Y	
6.5.2	Inadvertent operation	Y	Y	Y	Y	Y	
6.5.3	Status information	P/A[8]	Y	Y	P/A[8]	Y	[8])Only bullet b4. is applicable to unmanned system
6.5.4	Safe shutdown and failure tolerance requirements	N/A	Y	Y	N/A	Y	
6.5.5	Electronic, electrical, electromechanical components	Y	Y	Y	Y	Y	
6.5.6	Software functions						
6.5.6.1	Software criticality	Y	Y	Y	Y	Y	
6.5.6.2	Analysis of safety-critical software	Y	Y	Y	Y	Y	
6.5.6.3	Evaluation of software criticality	Y	Y	Y	Y	Y	
6.5.6.4	Software development	Y	Y	Y	Y	Y	
6.6	Operational safety						
6.6.1	Basic requirements	N/A	P/A	Y	N/A	Y	
6.6.2	Flight operations and mission control						
6.6.2.1	Launcher operations	N/A	N/A	N/A	Y	Y	
6.6.2.2	Contamination	Y	Y	Y	Y	Y	
6.6.2.3	Flight rules	N/A	N/A	Y	N/A	Y	
6.6.2.4	Hazardous commanding control	P/A [9]	Y	Y	P/A [9]	Y	[9]) Applicable to unmanned system before lift-off
6.6.2.5	Mission operation change control	N/A	Y	Y	N/A	Y	
6.6.2.6	Safety surveillance and anomaly control	N/A	Y	Y	N/A	Y	
6.6.2.7	Hazardous debris, fallout and impact control	N/A	N/A	N/A	Y	Y	
6.6.3	Ground operations						
6.6.3.1	Applicability	Y	Y	Y	Y	Y	
6.6.3.2	Initiation	Y	Y	Y	Y	Y	
6.6.3.3	Review and inspection	Y	Y	Y	Y	Y	
6.6.3.4	Hazardous operations	Y	Y	Y	Y	Y	
6.6.3.5	Launch and landing site	N/A	N/A	N/A	Y	Y	
6.6.3.6	Ground support equipment	Y	Y	Y	Y	Y	
7	**Safety analysis requirements and techniques**						
7.1	Overview	Non-normative					
7.2	General	Y	Y	Y	Y	Y	
7.3	Assessment and allocation of requirements						
7.3.1	Safety requirements	Y	Y	Y	Y	Y	
7.3.2	Additional safety	Y	Y	Y	Y	Y	

Clause	Headline	Un-manned space system		Manned space system	Launch vehicle		Remarks
		Satellite	Safety critical systems		for un-manned space-craft	for manned space-craft	
	requirements						
7.3.3	Define safety requirements - functions	Y	Y	Y	Y	Y	
7.3.4	Define safety requirements - subsystems	Y	Y	Y	Y	Y	
7.3.5	Justification	Y	Y	Y	Y	Y	
7.3.6	Functional and subsystem specification	Y	Y	Y	Y	Y	
7.4	Safety analyses during the project life cycle	P/A	Y	Y [10]	P/A	Y [6]	[10]) As appropriate for the project
7.5	Safety analyses						
7.5.1	General	Y	Y	Y	Y	Y	
7.5.2	Hazard analysis	Y	Y	Y	Y	Y	
7.5.3	Safety risk assessment	N/A	Y [11]	Y [11]	N/A	Y [11]	[11]) Use of *probabilistic* safety risk assessment subject to specific project requirements
7.5.4	Supporting assessment and analysis						
7.5.4.1	General	N/A	P/A	P/A	N/A	P/A	As appropriate for the project
7.5.4.2	Warning time analysis	N/A	P/A	P/A	N/A	P/A	
7.5.4.3	Caution and warning analysis	N/A	P/A	P/A	N/A	P/A	
7.5.4.4	Common-cause and common-mode analysis	N/A	P/A	P/A	N/A	P/A	
7.5.4.5	Fault tree analysis	N/A	P/A	P/A	N/A	P/A	
7.5.4.6	Human error analysis	N/A	P/A	P/A	N/A	P/A	
7.5.4.7	Failure modes, effects and criticality analysis	N/A	P/A	P/A	N/A	P/A	
7.5.4.8	Zonal analysis	N/A	P/A	P/A	N/A	P/A	
8	**Safety Verification**						
8.1	General	Y	Y	Y	Y	Y	
8.2	Hazard reporting and review						
8.2.1	Hazard reporting system	Y	Y	Y	Y	Y	
8.2.2	Safety status review	Y	Y	Y	Y	Y	
8.2.3	Documentation	Y	Y	Y	Y	Y	
8.3	Safety verification methods						
8.3.1	Verification engineering and planning	Y	Y	Y	Y	Y	
8.3.2	Methods and reports	Y	Y	Y	Y	Y	
8.3.3	Analysis	Y	Y	Y	Y	Y	
8.3.4.3	Inspections						
8.3.4.1	General	Y	Y	Y	Y	Y	
8.3.4.2	Preflight inspections	P/A[12]	Y	Y	P/A[12]	Y	[12])Only bullet c. applicable to unmanned system
8.3.4.3	Inflight inspections	N/A	N/A	Y	N/A	N/A	
8.3.5	Verification and approval	Y	Y	Y	Y	Y	
8.4	Verification of safety-critical functions						

Clause	Headline	Un-manned space system		Manned space system	Launch vehicle		Remarks
		Satellite	Safety critical systems		for un-manned space-craft	for manned space-craft	
8.4.1	Validation	Y	Y	Y	Y	Y	
8.4.2	Qualification	Y	Y	Y	Y	Y	
8.4.3	Failure tests	Y	Y	Y	Y	Y	
8.4.4	Verification of design or operational characteristics	Y	Y	Y	Y	Y	
8.4.5	Safety verification testing	Y	Y	Y	Y	Y	
8.5	Hazard close-out						
8.5.1	Safety assurance verification	Y	Y	Y	Y	Y	
8.5.2	Hazard close-out verification	Y	Y	Y	Y	Y	
8.6	Declaration of conformity of ground equipment	Y	Y	Y	Y	Y	Only ground equipment
Legend: Y … YES (= applicable) P/A … Partially applicable N/A … Not applicable							
NOTE: GSE is part of the system considered here							

Annex G (informative) European legislation and 'CE' marking

G.1 Overview

'CE' Marking is a requirement that is applicable to virtually all products which are designed and intended for use on the Ground. This includes all Ground products and Ground Support Equipment (GSE) and in particular all EGSE and most MGSE.

It should be noted that the 'CE' standards in themselves do not ensure that a system is entirely safe and should be used in the context of 'additional safety analysis' as well as showing compliance to the minimum legal requirements.

G.2 CE mark

The 'CE' is a mark by the producer/supplier to show he has satisfied all applicable Directives for the safety of his product and is intended to allow the 'Free movement of Goods' within the European Community. This requires compliance with European directives - generally through assessments to EN standards.

It is an offence to:

a. put a 'CE' mark on a product, without the supporting 'Technical File';

b. not to CE mark a product, if there is an applicable directive(s);

c. take a non-compliant product 'into service' anywhere within the European Community.

CE Marking is applicable to all Ground products including GSE regardless of whether it is being passed to a third party, a customer or designed and built for internal Company use.

G.3 Responsibility of the design authority

It is the responsibility of the 'Design Authority' to identify all directives which apply to the product design and to ensure assessment and compliance of the product(s) to the most recent edition of all applicable directives, legislation and relevant EN standards.

The 'Design Authority' is required to:

a. Identify all applicable directives;

b. Demonstrate technical compliance;

c. Hold a 'Technical File' for 10 years;

d. Issue a 'Declaration of Conformity', a User Manual with safety warnings and put the 'CE' mark on the product.

G.4 Declaration of conformity

The 'Declaration of Conformity' is a Legal statement by the Design Authority that the 'Essential Health & Safety Requirements' of all applicable directives for the product(s) have been satisfied and is issued only when documents showing compliancy are in place and before dispatch of the product or 'putting into service'.

G.5 References

The references below are provided to assist with CE assessment. The list is not exhaustive and is provided as general guidance for the directives which typically apply to the majority of space related ground products. In the majority of cases, 'CE' compliance can be declared by the 'Self Declaration' route, thus avoiding the need to involve any third party Certification Bodies.

a. All Electrical Ground Support Equipment (EGSE) and electrical systems or equipment used in Ground stations conform to the Low Voltage directive (LVD), (2006/95/EC) and the EMC directive (2004/108/EC). This is usually demonstrated by evaluation and testing to the most appropriate EN standards, typically EN 61010 (LVD) and EN 61326 (EMC).

b. Most Mechanical Ground Support Equipment (MGSE) falls within the scope of the Machinery directive (2006/42/EC), i.e. equipment with hazards due to moving parts, mobility and/or lifting or a lifting accessory. These are evaluated with respect to 'The Essential Health & Safety Requirements', given in Annex 1 of Appendix 1 of the directive.

c. GSE having pressure circuits and all Pressure Ground Equipment and Ground Support Equipment (PGSE) needs to be evaluated for applicability against the Pressure Equipment directive (PED) (97/23/EC) for Ground systems working at a pressure in excess of 0,5 bar.

d. Terminal Equipment needs to be evaluated for applicability of the Radio & Telecommunications Terminal Equipment (R&TTE) directive (1999/5/EC) for terminal equipment, often found in Ground Stations.

e. Apparatus to be used in explosive atmosphere conform to directive 94/9/CE.

f. Other European directives that need to be evaluated for applicability include:

1. Restriction of certain Hazardous Substances (RoHS) directive (2002/95/EC), which applies to some ground equipment and has an indirect impact on Flight Products, due to non-availability of some banned substances.

2. Waste Electrical & Electronic Equipment (WEEE) directive (2002/96/EC) applies to electrical products such as modems and EGSE.

g. All future Legislation and European directives should be evaluated and applied if applicable to the product.

Bibliography

ECSS-S-ST-00	ECSS system – Description and implementation and general requirements
ECSS-Q-ST-30-02	Space product assurance — Failure modes, effects, and criticality analysis (FMECA)
ECSS-Q-ST-40-02	Space product assurance – Hazard analysis
ECSS-Q-ST-40-12	Space product assurance — Fault tree analysis, Adoption notice ECSS/IEC 61025
IEC 50:1992	Electricity, electronics and telecommunications multilingual dictionary
ISO 14620-1:2002	Space systems — Safety requirements — Part 1: System safety